Safety Science 47 (2009) 1332–1336

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Cascade-based attack vulnerability on the US power grid

Jian-Wei Wang *, Li-Li Rong

Institute of System Engineering, Dalian University of Technology, 2 Ling Gong Rd., Dalian 116024, Liaoning, PR China

ARTICLE INFO

Article history:
Received 20 November 2008
Received in revised form 15 January 2009
Accepted 5 February 2009

Keywords:
Cascading failure
Attack
US power grid
Critical threshold
Tunable parameter

ABSTRACT

The vulnerability of real-life networks subject to intentional attacks has been one of the outstanding challenges in the study of the network safety. Applying the real data of the US power grid, we compare the effects of two different attacks for the network robustness against cascading failures, i.e., removal by either the descending or ascending orders of the loads. Adopting the initial load of a node j to be $L_j = [k_j(\Sigma_{m\in\Gamma_j} k_m)]^\alpha$ with k_j and Γ_j being the degree of the node j and the set of its neighboring nodes, respectively, where α is a tunable parameter and governs the strength of the initial load of a node, we investigate the response of the US power grid under two attacks during the cascading propagation. In the case of $\alpha < 0.7$, our investigation by the numerical simulations leads to a counterintuitive finding on the US power grid that the attack on the nodes with the lowest loads is more harmful than the attack on the ones with the highest loads. In addition, the almost same effect of two attacks in the case of $\alpha = 0.7$ may be useful in furthering studies on the control and defense of cascading failures in the US power grid.

1. Introduction

Recently, the resilience of real-world networks (Albert et al., 2000; Albert and Barabási, 2002; Holme et al., 2002; Strogatz, 2001; Newman, 2003; Goh et al., 2002) subject to random or intentional attacks has been one of the most central topics in network safety. Many real-world networks such as the Internet, the electrical power grid, the transportation networks, and so on, are robust to random attacks but vulnerable to intentional attacks. Evidence has demonstrated that in such networks, even though intentional attacks and random failures emerge very locally, the entire network can be largely affected, even resulting in global collapse. Typical examples include several blackouts in some countries, e.g., the largest blackout in US history took place on 14 August 2003 and the Western North American blackouts in July and August 1996, and the Internet collapse caused by congestion, e.g., a typical example is recent Internet collapse caused by the submarine earthquake near Taiwan in December 2006. These severe incidents have been attributed to cascading behaviors, and have been extensively explored.

Wu et al. (2008) studied the onset and spreading of cascading failure on weighted heterogeneous networks by adopting a local weighted flow redistribution rule, where the weight and tolerance of a node was correlated with its link degree k as k^θ and Ck^θ, respectively. Li et al. (2008) proposed a novel capacity model for complex networks against cascading failure, of which vertices with both higher loads and larger degrees were paid more extra capacities, i.e., the allocation of extra capacity on vertex i would be proportional to k_i^γ, where k_i was the degree of vertex i and $\gamma > 0$ was a free parameter. Motter and Lai (2002) proposed a new model for overload or congestion breakdown in the process of data packet transport on complex networks by assigning the capacity on a node. Holme et al. (2002) discussed overload breakdown in an evolving way and proposed a method to avoid such avalanches by using a global and dynamical searching algorithm. Crucitti et al. (2004) studied cascading failures by introducing efficiency dynamics. Simonsen et al. (2008) studied cascading failures in networks using a dynamical flow model based on simple conservation and distribution laws. It was found that considering the flow dynamics might imply reduced network robustness compared to previous static overload failure models. Bao et al. (2008) introduced the concept of load entropy, and then investigated the dynamics of load entropy during the failure propagation using a new cascading failures load model. Wang and Chen (2008) investigated universal robustness characteristic of weighted networks against cascading failure by adopting a local weighted flow redistribution rule, where the weight of an edge is $(k_i k_j)^\theta$ with k_i and k_j being the degrees of the nodes connected by the edge. In addition, a number of aspects of cascading failures have been discussed in some literatures, including the cascade control and defense strategy (Zhao and Gao, 2007; Sun et al., 2008; Motter, 2004; Wang and Kim, 2007; Ash and Newth, 2007), the model for describing cascade phenomena (Bao et al., 2008; Wang and Xu, 2004; Wu et al., 2007), the analytical calculation of capacity parameter (Wang et al., 2008; Wang and Rong, 2008; Zhao et al., 2004, 2005), and so on. In all cited studies above, one have focused only on the dynamic properties of the network showing that the removal of a group of nodes

* Corresponding author. Tel.: +86 411 81258693.
E-mail address: wdut@yahoo.cn (J.-W. Wang).

0925-7535/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2009.02.002

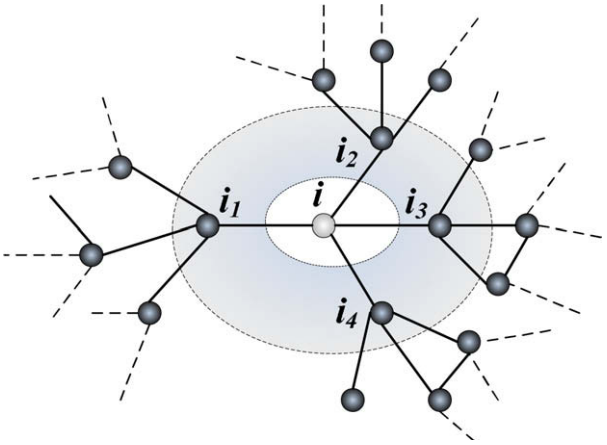

Fig. 1. The scheme illustrates the correlation between the initial load of a node i and its neighboring nodes, i.e., nodes i_1, i_2, i_3, and i_4.

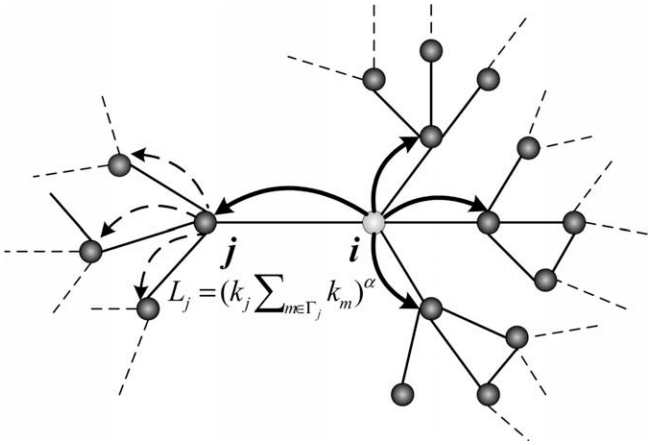

Fig. 2. The scheme illustrates the load redistribution triggered by an node-based attack. Node i is removed and the load on it is redistributed to the neighboring nodes connecting to node i. Among these neighboring nodes, the one with the higher load will receive the higher shared load from the broken node.

altogether can have important consequences. However, there are few works (Motter and Lai, 2002) about the effects of different attack strategies for the robustness against cascading failures on real-life networks.

In view of the importance of the study of attacks on real-life networks, which can be used either for protection in many infrastructure networks, e.g., in an electrical power grid, or for destruction in the spread of rumors and the control of epidemic diseases, we compare the effects of two attacks for the network robustness against cascading failures, i.e., the attacks of the nodes with the highest loads and the lowest loads, respectively. Adopting the famous US power grid, we numerically investigate the universal cascading phenomenon. Compared with the key role of the hub nodes of networks in many previous cascading studies, some interesting and counterintuitive results are found. It is expected that our findings will be helpful for real-life networks to protect the key nodes selected effectively and avoid cascading-failure-induced disasters.

2. The model

In all studies cited above, the load on a node (or an edge) was generally estimated by its degree or betweenness[1] and the redistribution load were usually forwarded following the shortest path. However, both load estimation and redistribution rules have their own drawbacks. Specially, the principle based on betweenness is reasonable only for small or medium-sized networks due to the requirement of structural information of the whole networks; while the principle based on node degree outweighs by its simplicity, but is inferior owing to its only consideration of single node degree, which loses much information thereby restricting many actual applications. Therefore, how to balance the complexity and the information quantity is a significant topic.

To reduce the complexity of the betweenness and improve the practicability of the degree, we present a new measure to assign the initial load of a node (see Fig. 1). Assume that the initial load L_j of a node j in the network is a function of the product of its degree k_j and the summation $\Sigma_{m\in\Gamma_j} k_m$ of the degrees of its neighboring nodes, and is defined as: $L_j = [k_j(\Sigma_{m\in\Gamma_j} k_m)]^{\alpha}$, where Γ_j represents the set of all neighboring nodes of the node j and α is a tunable parameter, which controls the strength of the initial load of a node. After a node i is attacked, its load will be redistributed to its neighboring nodes (see Fig. 2). The additional load ΔL_{ji} received by the node j is proportional to its initial load, i.e.,

$$\Delta L_{ji} = L_i \frac{L_j}{\sum_{n\in\Gamma_i} L_n} = L_i \frac{\left[k_j \Sigma_{m\in\Gamma_j} k_m\right]^{\alpha}}{\sum_{n\in\Gamma_i} [k_n \Sigma_{f\in\Gamma_n} k_f]^{\alpha}} \quad (1)$$

The capacity of a node is the maximum load that the node can handle. In man-made networks, the capacity is severely limited by cost. Thus, it is natural to assume that the capacity C_j of a node j is proportional to its initial load (Wu et al., 2008; Motter and Lai, 2002; Crucitti et al., 2004; Wang and Chen, 2008; Zhao and Gao, 2007; Sun et al., 2008; Motter, 2004; Wang et al., 2008; Wang and Rong, 2008; Zhao et al., 2004, 2005), i.e., $C_j = TL_j, j = 1, 2, 3, \ldots, N$, where the constant $T(\geqslant 1)$ is a tolerance parameter[2], and N is the number of nodes in the network. If $L_j + \Delta L_{ji} > C_j$, then the node j will be broken and induce further redistribution of flow $L_j + \Delta L_{ji}$ and potentially further breaking of other nodes. After the cascading process is over, we will calculate the number of broken nodes. To this end, we use CF_i to denote the avalanche size induced by removing node i. It is evident that $0 \leqslant CF_i \leqslant N - 1$. To quantify the attack-based robustness of the whole network, we adopt the normalized avalanche size, i.e.,

$$CF_{attack} = \frac{\sum_{i\in A} CF_i}{N_A(N-1)} \quad (2)$$

where A and N_A represents the set and the number of nodes attacked, respectively.

3. Analysis of attack strategies

In our cascading model, given a value of α, when the value of T is sufficiently small, we can imagine that it is easy for the

[1] The betweenness of a node can be obtained by counting the number of geodesics going it. More precisely, the betweenness b_i of a node i, sometimes referred to also as load, is defined as: $b_i = \sum_{j,k\in N, j\neq k} n_{jk}(i)/n_{jk}$, where n_{jk} is the number of shortest paths connecting j and k, while $n_{jk}(i)$ is the number of shortest paths connecting j and k and passing through i.

[2] In general, the more the load of a node, the stronger the capacity of the node. Therefore, considering the simplicity of a linear relationship and inspired by many cascading models cited above, we assume that all the nodes have the same tolerance parameter T. However, for a nonlinear relationship between the capacity and the load of some real complex networks, since it is very complicated and may further increase the frequency of overloads compared with a linear relationship, there is few works on exploring the impact on this model.

whole network to fully collapse in the case of an arbitrary node failure because the capacity of each node is limited. On the other hand, for sufficiently large T, since all nodes have the larger extra capacities to handle the load, no cascading failure occurs and the system maintains its normal and efficient functioning. Thus, with the increase of T, there should be some crossover behavior of the system from large scale breakdown to no breakdown, going through small scale ones. Therefore, inspired by many previous studies (Wu et al., 2008; Wang and Chen, 2008; Wang et al., 2008; Wang and Rong, 2008), we also use the crossover behavior to quantify the network robustness, i.e., the critical threshold T_c, at which a phrase transition occurs from normal state to collapse. When $T > T_c$, the system maintains its normal and efficient functioning; while when $T < T_c$, CF_{attack} suddenly increases from 0 and cascading failure emerges because the capacity of each node is limited, propagating the whole or part network to stop working. Therefore, T_c is the least value of protection strength to avoid cascading failure. Apparently, it is very important to investigate the effect of the other parameters for the critical threshold T_c.

Since few works discuss the role of different nodes of real-life networks in cascading failures, the aim of this paper is to compare the effects of different attacks for the network robustness against cascading failures. We adopt two simple attacks in our cascading model.

(1) Attack on the nodes with the highest loads (HL): a common attack strategy, used in the original study of computer networks, is to select the nodes in the descending order of loads in the network and then to remove nodes one by one starting from the node with the highest loads (if some nodes happen to have the same highest loads, we randomly choose one of them). In the heterogeneous networks, i.e., scale-free networks, the removal of the nodes with the highest loads is more likely to trigger cascading failures in general;
(2) Attack on the nodes with the lowest loads (LL): contrary to the strategy with HL, this attack strategy, rarely used to the real-life networks, is to select the nodes in the ascending order of loads in the network and then to remove nodes one by one starting from the node with the lowest load (if some nodes happen to have the same lowest loads, we randomly choose one of them).

In most previous studies, it was expected to undergo large-scale cascades if some vital nodes were attacked, but rarely in the case of random breakdown. As an example we consider the electrical power grid (Watts and Strogatz, 1998) of the western United States which has 4941 nodes and 6594 edges and discuss the effects of two attacks for the network robustness. To obtain an effect estimate of two attacks, we focus on the relationship between the critical threshold T_c and some parameters of our cascading model.

For each attack, we choose 50 nodes as the targeted ones attacked, and each simulation result is obtained by averaging over ten realizations of the electrical power grid of the western United States. According to the role of the tunable parameter α in adjusting the initial load of a node, we investigate the effects of two attacks in two cases[3] of $\alpha \leqslant 0.5$ and $\alpha > 0.5$.

Fig. 3 illustrates the normalized avalanche size CF_{attack} after cascading failures of all attacked nodes, as a function of the tolerance parameter T, for the electrical power grid of the western United States. It is original expected that the presence of a few nodes with larger loads has a disturbing side effect: the attack on the nodes with the highest loads may be prone to trigger a cascade of overload failures capable of disabling the network almost entirely than the attack on the ones with the lowest loads. However, as a result, our findings is on the contrary, i.e., the bigger cascades can be more likely to be triggered by the LL than by the HL when $\alpha \leqslant 0.5$, as shown in Fig. 3.

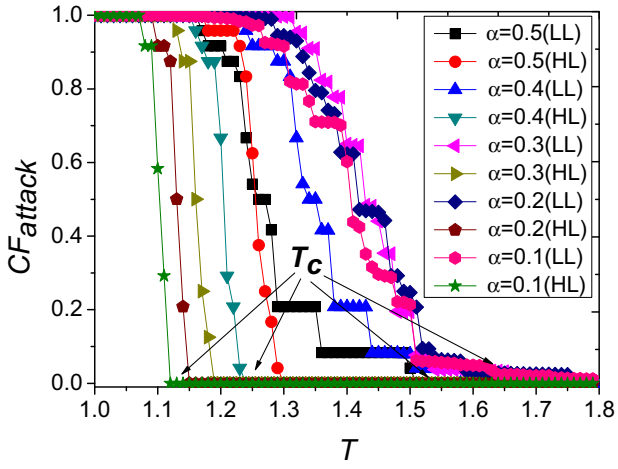

Fig. 3. Illustration of the relation between two attack strategies in the case of $\alpha \leqslant 0.5$.

We furthermore try to explain this counterintuitive phenomenon by adopting two sub-graphs of a network (see Fig. 4). Assume Fig. 4 to be two different parts of a network. When $\alpha = 0.2$, we compare the local effects of two attacks on nodes with the higher or lower loads for the network robustness. In order to avoid the breakdown of the neighboring nodes, we find that the lowest value of the capacity parameter α is 1.2872 and 1.5 in two cases of the failures of the nodes i and j in Fig. 4, respectively. Therefore, in this case the node with the lower loads plays more important in network safety than the one with the higher loads.

In Fig. 3, one can see: the bigger the value α, the smaller the difference of the effects of two attacks. In addition, as the value of the parameter α increases from 0.1 to 0.5, we can also see two interesting phenomena in our cascading model: on the one hand, the network robustness has a negative correlation with α under the HL (i.e., the estimate critical threshold T_c is positive correlation with α); while on the other hand, the network robustness has a positive correlation with α under the LL. Our finding has an important implication that it can provide guidance in protecting some nodes selected effectively to avoiding cascading-failure-induced disasters according to the different cases in real-life networks.

In the case of $\alpha > 0.5$, we also check the network robustness under two attacks in Fig. 5. It is easy to find two special point, i.e., $\alpha = 0.6$ and $\alpha = 0.7$. In the case of $\alpha = 0.6$, the HL is more effective than the LL in the bigger avalanche size of the broken nodes induced by cascading failures, while based on the obtained estimate T_c by CF_{attack}, the result is on the contrary. When $\alpha = 0.7$, the almost same T_c originating from two attacks is also different from many previous studies on cascading failures. In addition, when $\alpha > 0.7$, the HD is an efficient way to destruct the electrical power grid of the western United States.

We further investigate the relationship between the critical threshold T_c and the parameter α under two attacks. As shown in Fig. 6, switching of the efficiency of two attacks exists at the point of $\alpha = 0.7$.

[3] In our study, to accord with the positive proportion correlation between the initial load of a node j and $k_j(\Sigma_{m\in\Gamma_j} k_m)$, we set $\alpha > 0$. In addition, taking the impact of the product of k_j and $\Sigma_{m\in\Gamma_j} k_m$, we simply choose two ranges, i.e., $0 < \alpha \leqslant 0.5$ and $\alpha > 0.5$.

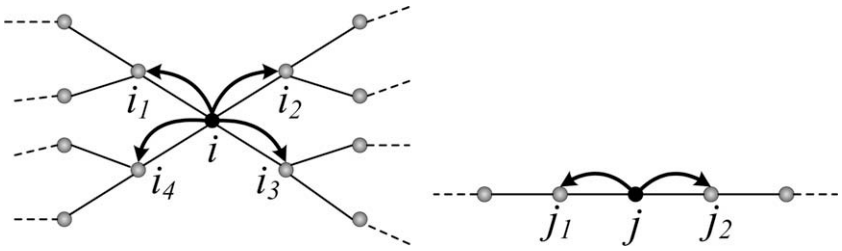

Fig. 4. A comparison between the effects of the breakdowns of two nodes with the higher (node i) or lower loads (node j) for theirs neighboring nodes, i_1, i_2, i_3, i_4, j_1, and j_2. For example, to avoid the failures of the neighboring nodes, it is found when $\alpha = 0.2$ that the lowest values of the capacity parameter T are 1.2872 and 1.5 in two cases of the removals of the nodes i and j, respectively, and the LL strategy is more likely to trigger cascading failures; when $\alpha = 1.2$, the lowest values of the capacity parameter T are 1.5743 and 1.5, respectively, and the HL strategy is harmful to disrupt the US power grid than the LL one.

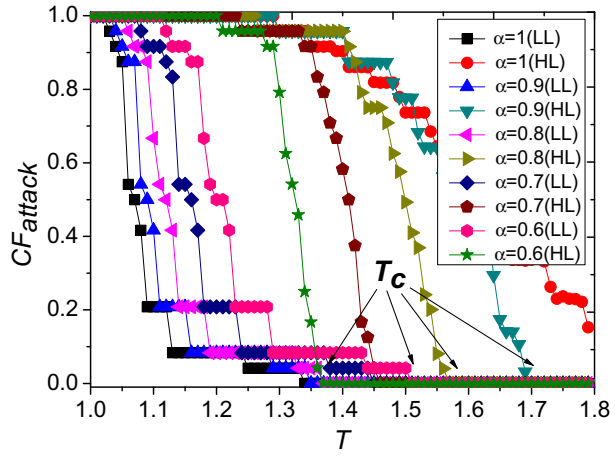

Fig. 5. Illustration of the relation between two attacks in the case of $\alpha \geqslant 0.6$.

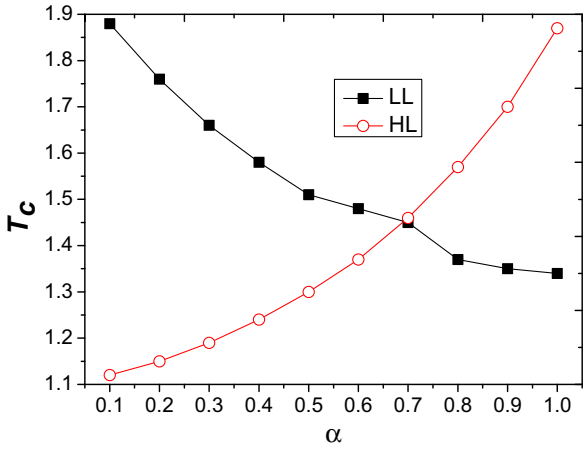

Fig. 6. Relation between the critical threshold T_c and the parameter α under two attacks.

4. Conclusion

In summary, adopting the local preferential redistribution rule of an overload node, we investigate the effects of two attack for the network robustness against cascading failures on the electrical power grid of the western United States. Assuming the initial load of a node j to be $L_j = [k_j(\Sigma_{m\in\Gamma_j} k_m)]^\alpha$ with k_j and Γ_j being the degree of the node j and the set of its neighboring nodes, respectively, where α is a tunable parameter and governs the strength of the node load, we numerically obtain the estimate for the network robustness under two attacks. Some interesting and counterintuitive results are found in our cascading model, of which an interesting finding is that the attack on the nodes with the lowest loads is a more effective may to destroy the electrical power grid of the western United States due to cascading failures when $\alpha < 0.7$. It is also found that the effects of two attacks are almost identical when $\alpha = 0.7$.

The study of attacks on complex networks is important in order to identify the robustness and vulnerability of real-life networks, which can be used either for protection in many infrastructure networks, e.g., in an electrical power grid, or for destruction in the spread of rumors and the control of epidemic diseases. Our work may have practical implications for protecting the key nodes selected effectively and avoid cascading-failure-induced disasters in the real world.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant Nos. 70571011 and 70771016.

References

Albert, R., Barabási, A.-L., 2002. Statistical mechanics of complex networks. Rev. Mod. Phys. 74, 47.
Albert, R., Jeong, H., Barabási, A.-L., 2000. Attack and error tolerance in complex networks. Nature 406, 387.
Ash, A., Newth, D., 2007. Optimizing complex networks for resilience against cascading failure. Physica A 380, 673.
Bao, Z.J., Cao, Y.J., Ding, L.J., Han, Z.X., Wang, G.Z., 2008. Dynamics of load entropy during cascading failure propagation in scale-free networks. Phys. Lett. A 372, 5778.
Bao, Z.J., Gao, Y.J., Ding, L.J., Wang, G.Z., Han, Z.X., 2008. Synergetic behavior in the cascading failure propagation of scale-free coupled map lattices. Physica A 387, 5922.
Crucitti, P., Latora, V., Marchiori, M., 2004. Model for cascading failures in complex networks. Phys. Rev. E 69, 045104.
Goh, K.-I., Kahng, B., Kim, D., 2002. Fluctuation-driven dynamics of the internet topology. Phys. Rev. Lett. 88, 108701.
Holme, P., Kim, B.J., Yoon, C.N., Han, S.K., 2002. Attack vulnerability of complex networks. Phys. Rev. E 65, 056109.
Li, P., Wang, B.H., Sun, H., Gao, P., Zhou, T., 2008. A limited resource model of fault-tolerant capability against cascading failure of complex network. Eur. Phys. J. B 62, 1.
Motter, A.E., 2004. Cascade control and defense in complex networks. Phys. Rev. Lett. 93, 098701.
Motter, A.E., Lai, Y.C., 2002. Cascade-based attacks on complex networks. Phys. Rev. E 66, 065102.
Newman, M.E.J., 2003. The structure and function of complex networks. SIAM Rev. 45, 167.
Simonsen, I., Buzna, L., Peters, K., Bornholdt, S., Helbing, D., 2008. Transient dynamics increasing network vulnerability to cascading failures. Phys. Rev. Lett. 100, 218701.
Strogatz, S.H., 2001. Exploring complex networks. Nature (London) 410, 268.
Sun, H.J., Zhao, H., Wu, J.J., 2008. A robust matching model of capacity to defense cascading failure on complex networks. Physica A 387, 6431.
Wang, W.X., Chen, G.R., 2008. Universal robustness characteristic of weighted networks against cascading failure. Phys. Rev. E 77, 026101.

Wang, B., Kim, B.J., 2007. A high-robustness and low-cost model for cascading failures. Europhys. Lett. 78, 48001.
Wang, J.W., Rong, L.L., 2008. Effect attack on scale-free networks due to cascading failures. Chin. Phys. Lett. 25, 3826.
Wang, X.F., Xu, J., 2004. Cascading failures in coupled map lattices. Phys. Rev. E 70, 056113.
Wang, J.W., Rong, L.L., Zhang, L., Zhang, Z.Z., 2008. Attack vulnerability of scale-free networks due to cascading failures. Physica A 387, 6671.
Watts, D.J., Strogatz, S.H., 1998. Collective dynamics of 'small-world' networks. Nature 393, 440.
Wu, J.J., Sun, H.J., Gao, Z.Y., 2007. Cascading failures on weighted urban traffic equilibrium networks. Physica A 386, 407.
Wu, Z.X., Peng, G., Wang, W.X., Chan, S., Wong, E.E.M., 2008. Cascading failure spreading on weighted heterogeneous networks. J. Stat. Mech., P05013.
Zhao, H., Gao, Z.-Y., 2007. Cascade defense via navigation in scale free networks. Eur. Phys. J. B 57(1), 95.
Zhao, L., Park, K., Lai, Y.C., 2004. Attack vulnerability of scale-free networks due to cascading breakdown. Phys. Rev. E 70, 035101 (R).
Zhao, L., Park, K., Lai, Y.C., Ye, N., 2005. Tolerance of scale-free networks against attack-induced cascades. Phys. Rev. E 72, 025104.